PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04B 10/00 — A2

(11) International Publication Number: WO 99/39464

(43) International Publication Date: 5 August 1999 (05.08.99)

(21) International Application Number: PCT/IL99/00044

(22) International Filing Date: 25 January 1999 (25.01.99)

(30) Priority Data:
123107 29 January 1998 (29.01.98) IL

(71) Applicant *(for all designated States except US)*: BEN-GURION UNIVERSITY OF THE NEGEV [IL/IL]; Research and Development Authority, P.O. Box 653, 84105 Beer Sheva (IL).

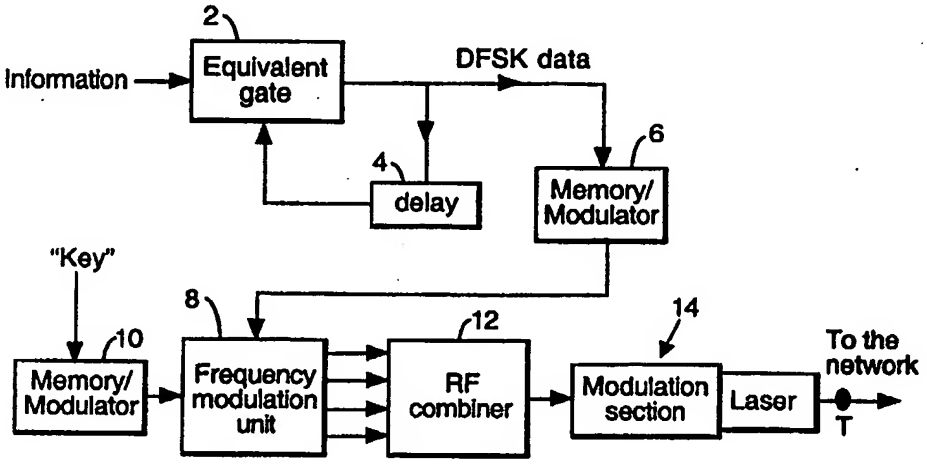
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SADOT, Dan [IL/IL]; 76965 Kfar Bilu 143 (IL). SHEM TOV, Dariush [IL/IL]; Allenby Street 85, 65134 Tel Aviv (IL).

(74) Agent: WOLFF, BREGMAN AND GOLLER; P.O. Box 1352, 91013 Jerusalem (IL).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: A SYSTEM AND A METHOD FOR INFORMATION SECURITY IN OPTICAL COMMUNICATION NETWORKS



(57) Abstract

The invention provides, in a system for effecting information security in an optical communication network, an optical data encryptor including first input means for receiving information signals to be transmitted over said communication network; a frequency-to-frequency coding means for coding the information received and for transforming the coded information into a stream of differential frequency shift keying (DFSK) signals; second input means for receiving key signals; a frequency modulation unit for receiving the DFSK stream and the key signals, for matching each signal of the DFSK stream with *m* key signals, and for dividing the matched stream into sets of *n* signals each, where *m* and *n* are positive integers; and a combiner for combining the sets, to be utilized for modulating optical transmitting means prior to effecting encrypted optical transmission over the communication network.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A SYSTEM AND A METHOD FOR INFORMATION SECURITY IN OPTICAL COMMUNICATION NETWORKS

Technical Field

The present invention relates to optical communication networks, and more particularly to a method and system for information security in optical communication networks.

Background Art

Even though it seems that optical communications will play a major role in future networks, surprisingly very few efforts are devoted to information security within optical systems. Computer coding and keying algorithms are currently being used regardless of the high-speed upgrade experienced by the communication links, a situation which may turn information security into a severe bottleneck in future networks.

The optical encryption principle according to the present invention is based upon dual transmission of two data streams over the same optical carrier. By combining modulations in a very similar fashion, e.g., frequency shift keying (FSK) together with differential phase shift keying (DPSK) or double FSK streams, the modulations modify the instantaneous phase of the optical carrier. With the absence of a prior knowledge of the key stream and its parameters, the two data streams will bury each other within the optical carrier phase. Other combinations involving amplitude shift keying (ASK) together with phase shift keying (PSK) are not beneficial for data encryption since they affect different physical quantities (wave amplitude together with phase), resulting in a low encryption level.

Disclosure of the Invention

It is therefore a broad object of the present invention to provide a method and a system for effecting information security in an optical communication network, utilizing combined modulation formats over the same optical carrier of both the information and the key.

In accordance with the present invention, there is therefore provided a system for effecting information security in an optical communication network, said system

comprising an optical data encryptor including first input means for receiving information signals to be transmitted over said communication network; a frequency-to-frequency coding means for coding the information received and for transforming the coded information into a stream of differential frequency shift keying (DFSK) logic signals; second input means for receiving key bits; a frequency modulation unit for receiving said DFSK stream and said key bits, for matching each bit of said DFSK stream with a pair of key bits, and for dividing the matched stream into sets of n bits each, where n is a positive integer; and a combiner for combining said sets, to be utilized for modulating optical transmitting means prior to effecting encrypted optical transmission over said communication network.

The invention further provides a method for effecting information security in an optical communication network, said method comprising frequency-to-frequency coding of information to be secured by matching each bit of information in a data stream with a pair of key bits to produce a coded information data stream; time-to-frequency coding of said data stream by transforming said data stream into a differential frequency shift keying (DFSK) stream, and dividing said DFSK stream into sets of n bits each, to be simultaneously transmitted over said communication network.

Brief Description of the Drawings

The invention will now be described in connection with certain preferred embodiments with reference to the following illustrative figures so that it may be more fully understood.

With specific reference now to the figures in detail, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of the preferred embodiments of the present invention only, and are presented in the cause of providing what is believed to be the most useful and readily understood description of the principles and conceptual aspects of the invention. In this regard, no attempt is made to show structural details of the invention in more detail than is necessary for a fundamental understanding of the invention, the description taken

with the drawings making apparent to those skilled in the art how the several forms of the invention may be embodied in practice.

Fig. 1 is a block diagram of a double security level data encryptor/transmitter in an information security system according to the present invention;

Fig. 2 is a block diagram of a double security level data decryptor/receiver in an information security system according to the present invention;

Fig. 3 illustrates plots showing experimental computer results, using the security method of the present invention;

Fig. 4 illustrates plots showing experimental computer results, assuming added white Gaussian noise;

Fig. 5 illustrates a computer experiment and theoretical curves, assuming added Gaussian noise of BER vs SNR at point R′ of the receiver of Fig. 2;

Fig. 6 is a block diagram of a combined modulation FSK/DPSK optical encryptor-transmitter according to the present invention;

Fig. 7 is a block diagram of a DPSK coherent receiver;

Fig. 8 is a plot illustrating impact of the DPSK-related phase noise on the FSK demodulated signal;

Fig. 9 is a plot illustrating impact of frequency noise on the DPSK signal, observed at the frequency domain;

Fig. 10 is a block diagram of a decryptor/receiver;

Fig. 11 is a block diagram of a further embodiment of an encryptor/transmitter according to the present invention, and

Fig. 12 is a block diagram of a further embodiment of a decryptor/receiver according to the present invention.

Detailed Description

The present invention may be carried out utilizing either digital or analog processing and communication techniques. For better understanding, a specific example of encryption of information, utilizing a digital communication technique according to the present invention, will now be described.

Seen in Fig. 1 is a data encryptor/transmitter according to a preferred embodiment of the present invention utilizing a digital technique, having two inputs: an information input and a key data streams input. The information input is applied to an equivalent gate 2 governed by a bit delay 4 for differential encoding and is then passed to a memory/modulator 6, arranging the DFSK information stream into four-bits sets before it is fed to a frequency modulation unit 8. The key data stream input is applied to memory/modulator 10, which arranges it into eight-bits sets before applying it to the frequency modulation unit 8.

According to Table 1 below, the two memories/modulators 6 and 10 modulate n (e.g., four) voltage control oscillators (VCOs, not shown), forming n frequency shift keying (FSK) subcarrier frequencies. In turn, after passing the frequencies through the RF combiner 12 to be combined, the four-bits FSK/DFSK signal amplitude is utilized to modulate an optical transmission means, e.g., a high speed laser 14, and the modulated laser beam is transmitted to the optical network. To overcome an electronic bottleneck, it is possible to utilize an all-optical encoding scheme by replacing the single laser and the n electronic VCOs with a $1 \times n$ array of laser transmitters, forming a dense wavelength division multiplexing (WDM) signal.

By using combined modulation formats of both the information and key data streams over the same optical carrier and in a very similar fashion, both data streams are mixed. It is then possible to extract the modulated data only with a prior knowledge of the key parameters.

A double security level is achieved by using frequency-to-frequency, together with time-to-frequency, coding algorithms. In frequency-to-frequency coding, each bit of information is matched to a pair of key bits, together forming 2^3 possible transmission frequencies. The frequency map used is presented in the following Table 1:

TABLE 1. FSK/DFSK Code Map

Logic Data Value	1	0	0	0	0	1	1	1
Logic Key Value	00	00	01	10	11	01	10	11
Frequency #	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8

In time-frequency coding, the information data stream is transformed into a DFSK stream, which in turn is divided into four-bits sets. Each set is simultaneously transmitted, according to the frequency map of the above Table 1. Consequently, a double security level is achieved, as follows:

(i) It is unknown which frequency is related to either logic 1 or 0, e.g., binary 1 or 0.

(ii) Sets of four bits are simultaneously transmitted, resulting in an unknown bits order, which is crucial for DFSK demodulation. Furthermore, the key for bit reordering changes from set to set, according to the key data stream.

The transmitted signal can be mathematically described by the equation:

$$DFSK\ /\ FSK = \sum_{n=0_i=1}^{N}\sum^{4} \cos\left[2\pi\left(f_0 + f_{sc} + \hat{k}_{4n+i}\cdot df_0 + k_{4n+i}\cdot df_1 + z_{8n+2i}\cdot df\right)t\right]\cdot \left[u\left(t-4T_b n\right) - u\left(t-4T_b\left(n+1\right)\right)\right] \quad (1)$$

wherein:

$u(\cdot)$ is a unit step function;

f_0 is the optical carrier frequency;

f_{sc} is the subcarrier frequency;

df_0 and df_1 are constant frequency shifts, according to the information logic value 0 or 1, respectively;

k and $\hat{k}$ are the information binary value and its binary complement, respectively;

z is the decimal value of each pair of key bits;

df is a frequency shift multiplier;

T_b is the information bit duration; and

$4n$ is the total number of information bits.

Referring now to Fig. 2, which illustrates a preferred embodiment of an optical data decryptor/receiver according to the present invention utilizing a digital communication technique, there is shown an optical arrangement 16 for receiving the modulated optical beam from the network as transmitted by the transmitter and for applying signals representing the received optical beam to an RF splitter 18, where they are split into two branches 20, 22. The upper and lower branches 20, 22 demultiplex the data related to logics 1 and 0 in demultiplexer units 24, 26, respectively, according to prior knowledge of the key. This is implemented by frequency multiplication between one of the n RF generated signals (the inputs to each of multiplexer units 24, 26) which is selected according to the key information at the multiplexer units, with the received signals in each branch 20 and 22, respectively. In turn, the resulting signals at either of the outputs of the mixers 28, 30 are advantageously fed through a bandpass filter (BPF) 32, 34, eliminating high-order harmonics of the multiplied signals, and eliminating most of the added white noise, thus improving the received sensitivity. The output signal at each BPF 32, 34 is the original DFSK signal with no encryption, at the original frequency f_2 or f_1, for example according to binary values 0 or 1, at the higher and lower branches, respectively. The data streams from the two branches are combined at the RF combiner 36 and applied to a DFSK demodulator 38, reconstructing the original information.

Computer experiments of the double security level system were carried out, the results of which are presented in Figs. 3 to 5. A four-bit set of original information, and the encoded FSK/DFSK stream after the first security level (only a theoretical plot, since it cannot be measured) are depicted in Figs. 3a and 3b, respectively. The simultaneously transmitted four-bits set after the second security level (point T at the output of the transmitter of Fig. 1), and the reconstructed DFSK data (point R at the receiver of Fig. 2) are depicted in Figs. 3c and 3d, respectively.

Similar to Fig. 3, Figs. 4a to 4d present the results of a computer experiment which included additive white Gaussian noise. In this example, the received signal to

noise ratio (SNR) at point R′ at the receiver, is 20 dB. Perusal of Figs. 4c and 4d reveals that the BPFs 32, 34 at the receiver essentially eliminate most of the additive white noise, thus significantly improving the receiver sensitivity.

Fig. 5 shows computer experiment (circles) and theoretical (continuous) bit error ratio (BER) curves versus received SNR (at point R′ of the receiver in Fig. 2). Assuming additive Gaussian noise, the required SNR for 10^{-9} BER is less than 25 dB.

For 10K information bits and 20K key bits, the number of possible combinations per set is 4!=24, and the total number of combinations is $24^{(10,000/4)} = 10^{100}$. Assuming 10^{10} calculations per second and 10% of realistic combinations, the required calculation time for ineligible information decoding is 10^{8} years.

The embodiments described hereinbefore with reference to Figs. 1 to 5, relating to FSK-FSK combined modulation format, provide a practical example that can be implemented using incoherent direct-detection systems, as are most of the commercial optical communication systems. However, combined modulation can include phase shift keying (PSK) together with FSK, or differential PSK (DPSK) together with FSK, as well as other combinations involving frequency and phase modulations. In that case, to recover the phase information, coherent (rather than direct detection) systems are required. This is more difficult to implement, but can offer higher security level. A detailed example for an FSK-DPSK scheme will now be described with reference to Figs. 6 to 10.

An FSK-DPSK encryptor/transmitter is illustrated in Fig. 6. A semiconductor DFB laser 40 having an active region 42 and a grating 44 is used as a transmitter. The FSK data stream 46 modulates the frequency selective grating 44 and converts the modulating signal voltage into a frequency modulated optical signal. The output beam 48 is, in turn, externally DPSK-modulated with data 50 using an LiNbO3 phase modulator 52. The resulting optical signal 54 is both FSK and DPSK dual-modulated. The transmitted signal can be mathematically described by:

$$DFSK / FSK = \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \cos\left[\left(\omega_o + k_{ij}\Delta\omega\right)t + \left(s_i + 1\right)\pi\right] \cdot \left[u\left(t - \langle Mi + j\rangle T_{kb}\right) - u\left(t - \langle Mi + J + 1\rangle T_{kb}\right)\right] \quad (2)$$

wherein:

$u(\cdot)$ is a unit step function;

ω_o is the optical carrier frequency;

$\Delta\omega$ is the FSK frequency shift;

$k_{i,j}$ and S_i are FSK (key) and DPSK (data) binary values, respectively;

T_{kb} is the key bit duration;

M is the total number of key bits during T_b; and

N is the total number of information bits.

Both modulating signals act on the same optical phase independently and therefore bury each other. By using an optical-to-electrical conversion (either direct- or coherent-detection), neither of the signals can be reconstructed. Thus, the optically transmitted information is considered completely secured.

A preferred embodiment of a DPSK coherent light receiver block diagram is illustrated in Fig. 7. FSK/DPSK data, together with signals from a local oscillator laser 56, is directly fed via an optical coupler 58 and a photodetector 59 to a mixer 60 through a first branch 62 and simultaneously to the mixer 60 via a delay 64 through a second branch 66.

Without modulation, the signal at the output of the mixer 60, at point m, is:

$$X_{mixed} = A\cos\left(\omega_{IF}t\right)\cos\left(\omega_{IF}\left(t + \tau\right)\right) \quad (3)$$

wherein:

ω_{IF} is the intermediate frequency after the mixing between the signal and local oscillator;

τ is the delay time; and

A is the amplitude of the mixed signal.

After the lowpass filter (LPF) 68, the signal output is:

$$X_{output} = \frac{A}{2}\cos(\omega_{IF}\tau).$$

(4)

For optimal DPSK demodulation, the delay time is set to $\tau = T_b$, wherein T_b is the data bit duration. When the DPSK modulation is on, the mixed IF signal (point *m* of Fig. 7) is:

$$X_{mixed} = \sum_{i=0}^{N-1} A\cos(\omega_{IF}t + \langle s_i + 1\rangle\pi)\cos\{\omega_{IF}(t + T_b) + (s_{i+1} + 1)\pi\} \cdot \left[u(t - iT_b) - u(t - \langle i + 1\rangle T_b)\right]$$

(5)

and after the LPF 68, the signal output becomes:

$$X_{output} = \sum_{i=0}^{N-1} \frac{A}{2}\cos\{\omega_{IF}T_b + (s_{i+1} - s_i)\pi\} \cdot \left[u(t - iT_b) - u(t - \langle i + 1\rangle T_b)\right].$$

(6)

Accordingly, the DPSK demodulation is obtained by utilizing a simple decision gate related to an appropriate threshold. For example, by setting $\omega_{IF}T_b = 2k\pi$, where k is any integer, and setting the threshold to zero, the decision rule will be the following:

$$\begin{cases} X_{output} \geq 0 \rightarrow s_i = s_{i+1} \\ X_{output} < 0 \rightarrow s_i \neq s_{i+1} \end{cases}$$

(7)

When both the combined FSK (key) and DPSK (data) modulations are on, the phase of the IF carrier will change, according to the FSK modulation depth and modulating frequency. The DPSK-related phase changes can be regarded as phase noise imposed on the FSK signal, as illustrated in Fig. 8.

Similarly, the FSK-related frequency changes can be regarded as frequency noise imposed on the DPSK signal, as illustrated in Fig. 9. The impact of FSK modulation on the DPSK signal can be analyzed by replacing Equation 5 with

$$X_{mixed} = \sum_{i=0}^{N-1}\sum_{j=0}^{M-1} A\cos\left[\left(\omega_{IF} + k_{ij}\Delta\omega\right)t + \left(s_i + 1\right)\pi\right]\cos\left[\left(\omega_{IF} + k_{i+1,j}\Delta\omega\right)\left(t + T_b\right) + \left(s_{i+1} + 1\right)\pi\right]\cdot$$
$$\left[u\left(t - \langle Mi + j\rangle T_{kb}\right) - u\left(t - \langle Mi + j + 1\rangle T_{kb}\right)\right]$$

(8)

The frequency variance due to the FSK modulation can be designed in such a way that the DPSK data will be totally buried. Consequently, after the LPF 68, the signal output is obtained by replacing equation 6 with

$$X_{output} = \sum_{i=0}^{N-1}\sum_{j=0}^{M-1} \frac{A}{2}\cos\left\{\omega_{IF}T_b + \left[\left(k_{i+1,j} - k_{i,j}\right)\Delta\omega t + k_{i+1,j}\Delta\omega T_b\right] + \left(s_{i+1} - s_i\right)\pi\right\}\cdot$$
$$\left\{u\left(t - \langle Mi + j\rangle T_{kb}\right) - u\left(t - \langle Mi + j + 1\rangle T_{kb}\right)\right\}$$

(9)

Equation (9) forms the final expression for the combined FSK/DPSK non-decryptable detected signal. It is clear that the recovered DPSK data stream does totally depend on the FSK key data, as appearing in the square parenthesis on the right hand side of Equation (9). With an appropriate design of the FSK key data and its parameters, e.g., frequency and modulation depth $\Delta\omega$, the DPSK data will be totally buried and unrecoverable. Furthermore, the FSK key data can use pseudo-random sequences of any required length and of any bit rate in relation to the data stream bit rate $\frac{1}{T_b}$.

By obtaining the FSK key data, the eligible user can inversely FSK modulate the received optical signal in order to cancel the phase distortions that were imposed by the key data stream. The remaining signal can, in turn, be DPSK demodulated with no distortions. The decrypted receiver block diagram is illustrated in Fig. 10. As shown, the FSK key data 70 is fed to a multiplexer 72 for multiplexing between the frequency shift $\Delta\omega$ and the DC value. After multiplying the received FSK/DPSK data stream with the multiplexer output signal in mixer 74, the resulting signal at the mixer output at point p is inversely FSK modulated, and the original DPSK data is obtained. The inverse FSK modulation process can be understood by observing the

signal spectrum in Fig. 9. For each frequency shift which is generated by the original FSK modulation at the DFB laser transmitter, there will be an inverse shift at the decrypted receiver by multiplication, in the RF domain, between the received FSK/DPSK signal and the multiplexer output of Fig. 10. In turn, the resulting DPSK signal at point *p* can be further DPSK modulated, according to Equations 5 to 7.

Another embodiment of the invention using digital techniques and components, except for the modulation and demodulation of the optical information, is illustrated in Figs. 11 and 12. Seen in Fig. 11 is an optical demodulator 76 receiving optically modulated data from an optical link and demodulating the data into discrete (digital) levels. The demodulated data is then passed through a serial to parallel converter 78 to a bit manipulator 80 and a differential coder 82, to be differentially encoded in *N* bit blocks. The key data stream generated at 84 is transferred to the frequency modulation unit 86, composed of a frequency allocation table 88 and a frequency synthesizer 90, allocating RF frequencies for transmission according to the differentially encoded data, key stream and frequency allocation table. The modulated frequencies are passed on via a combiner 92 to a laser 94, to be transmitted through an optical link.

The receiver illustrated in Fig. 12 receives optical signals from a link, passes the signals via a splitter 96 to a multi-channel front end 98 and then to a frequency demodulation unit 100, composed of a spectrum evaluator 102 and a frequency allocation table 104. Data from the key generator 106 is passed through the frequency allocation table 104 to the differential decoder 108, the bit manipulator 110 and the parallel to series converter 112 for extracting the original data stream and for passing same to the laser 114, to be transmitted via an optical link.

Thus, data from the optical link is received at the encryption transmitter sub-system, and in turn, is treated in *N* bit blocks. Each *N* bit block is processed in real-time and then transmitted back to the optical layer. At the transmitter, each bit of the block is differentially encoded and then encrypted according to the frequency allocation table. At the receiver side, after passing through the optical link, the received data is treated in *M* nsec periods. Every *M* nsec, the spectrum at the receiver's front end is evaluated, demodulated and fed in *N* bit blocks according to a reverse frequency allocation table,

and in turn, into a differential decoder. Both processes of encryption/decryption implemented at the transmitter/receiver, respectively, are key and differential code-related. Thus, the differential coding, followed by key generation at the transmitter, is related (in a reverse order) to differential decoding and key generation at the receiver.

It will be evident to those skilled in the art that the invention is not limited to the details of the foregoing illustrated embodiments and that the present invention may be embodied in other specific forms without departing from the spirit or essential attributes thereof. The present embodiments are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than by the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

CLAIMS:

1. In a system for effecting information security in an optical communication network, an optical data encryptor comprising:

first input means for receiving information signals to be transmitted over said communication network;

a frequency-to-frequency coding means for coding the information received and for transforming the coded information into a stream of differential frequency shift keying (DFSK) signals;

second input means for receiving key signals;

a frequency modulation unit for receiving said DFSK stream and said key signals, for matching each signal of said DFSK stream with *m* key signals, and for dividing the matched stream into sets of *n* signals each, where *m* and *n* are positive integers; and

a combiner for combining said sets, to be utilized for modulating optical transmitting means prior to effecting encrypted optical transmission over said communication network.

2. The system as claimed in claim 1, further comprising an optical data decryptor, said decryptor including:

a signal splitter for receiving signals representing said encrypted optical transmission and for splitting said signals into a first branch containing data related to a first signal level and a second branch containing data related to a second signal level;

a first and a second demultiplexers for demultiplexing the data in each of said first and second branches, in accordance with the data of said key signals;

combining means for combining the demultiplexed first and second signals of said branches, and

a DFSK demodulator for reconstruction of said information signals.

3. The system as claimed in claim 1, wherein said first input means comprises an equivalent gate governed by a delay signal and a first memory/modulator.

4. The system as claimed in claim 1, wherein said second input means comprises a second memory/modulator.

5. The system as claimed in claim 1, wherein said optical transmitting means comprises a high speed laser including a modulator.

6. The system as claimed in claim 2, further comprising a bandpass filter connected in each branch between said demultiplexer unit and said combining means.

7. The system as claimed in claim 2, further comprising an optical arrangement for receiving a transmitter modulated optical beam from the communication network and for applying signals corresponding to said modulated beam to said splitter.

8. In a system for effecting information security in an optical communication network, an optical data encryptor, comprising:

a semiconductor DFB laser having an active region and a grating for receiving frequency shift keying (FSK) key data and producing frequency modulated optical key signals, and

a semiconductor phase modulator receiving said optical key signals and phase modulating the signals with DPSK modulated data stream to produce FSK and DPSK dual modulated encrypted signals to be optically transmitted over said communication network.

9. The system as claimed in claim 8, wherein said semiconductor phase modulator is a $LiNbO_3$ phase modulator.

10. The system as claimed in claim 8, further comprising an optical data decryptor, said decryptor comprising:

a mixer for receiving and mixing said FSK and DPSK dual modulated encrypted signals with said FSK key data multiplexed by a multiplexer to produce an output signal, and

a modulator for inversely FSK modulating said output signal for obtaining said DPSK data stream at the output thereof.

11. The system as claimed in claim 10, wherein said modulator comprises a first branch leading to a mixer and a second branch leading to said mixer via a delay unit.

12. The system as claimed in claim 11, further comprising a lowpass filter connected to the output of said mixer.

13. A method for effecting information security in an optical communication network, said method comprising:

frequency-to-frequency coding of information to be secured by matching each information signal unit in a data stream with *m* key signals to produce a coded information data stream;

time-to-frequency coding of said data stream by transforming said data stream into a stream of differential frequency shift keying (DFSK) logic signals, and

dividing said DFSK stream into sets of *n* signal units each, to be simultaneously transmitted over said communication network.

14. The method as claimed in claim 13, further comprising:

receiving said transmitted DFSK stream;

splitting said DFSK stream into a first branch and a second branch;

demultiplexing data related to a first signal level in said first branch and data related to a second signal level in said second branch, in accordance with the data of said key signals;

combining the demultiplexed signals of said first and second branches; and

reconstructing said information by demodulating the combined stream of DFSK signals.

15. The method as claimed in claim 13, further comprising filtering the demultiplexed signals in said first and second branches to eliminate high order harmonics of the multiplied signal and most of the white noise, prior to combining the filtered signals.

16. A method for effecting information security in an optical communication network, said method comprising:

encrypting information signals so as to conform with the equation:

$$DFSK / FSK = \sum_{n=0,i=1}^{N}\sum^{4} \cos\left[2\pi\left(f_0 + f_{sc} + \hat{k}_{4n+i}\cdot df_0 + k_{4n+i}\cdot df_1 + z_{8n+2i}\cdot df\right)t\right]\cdot$$

$$\left[u\left(t-4T_b n\right) - u\left(t-4T_b\left(n+1\right)\right)\right]$$

wherein:

$u(\cdot)$ is a unit step function;

f_0 is the optical carrier frequency;

f_{sc} is the subcarrier frequency;

df_0 and df_1 are constant frequency shifts, according to the information logic value 0 or 1, respectively;

k and $\hat{k}$ are the information binary value and its binary complement, respectively;

z is the decimal value of each pair of key bits;

df is a frequency shift multiplier;

T_b is the information bit duration; and

$4n$ is the total number of information bits.

17. A method for effecting information security in an optical communication network, said method comprising:

producing frequency modulated optical key signals (FSK) by frequency modulating a semiconductor DFB laser with key data, and

phase modulating said FSK signals with DPSK modulated data stream to produce FSK and DPSK dual-modulated encrypted signals to be optically transmitted over said communication network.

18. The method as claimed in claim 17, further comprising:

receiving said transmitted encrypted signals;

multiplexing said FSK key data;

mixing said FSK and DPSK dual-modulated encrypted signals with the multiplexed FSK key data to produce output signals, and

inversely modulating said output signals with said FSK signals to obtain said DPSK data stream.

19. The method as claimed in claim 18, further comprising filtering said obtained DPSK data stream through a lowpass filter.

Fig.1.

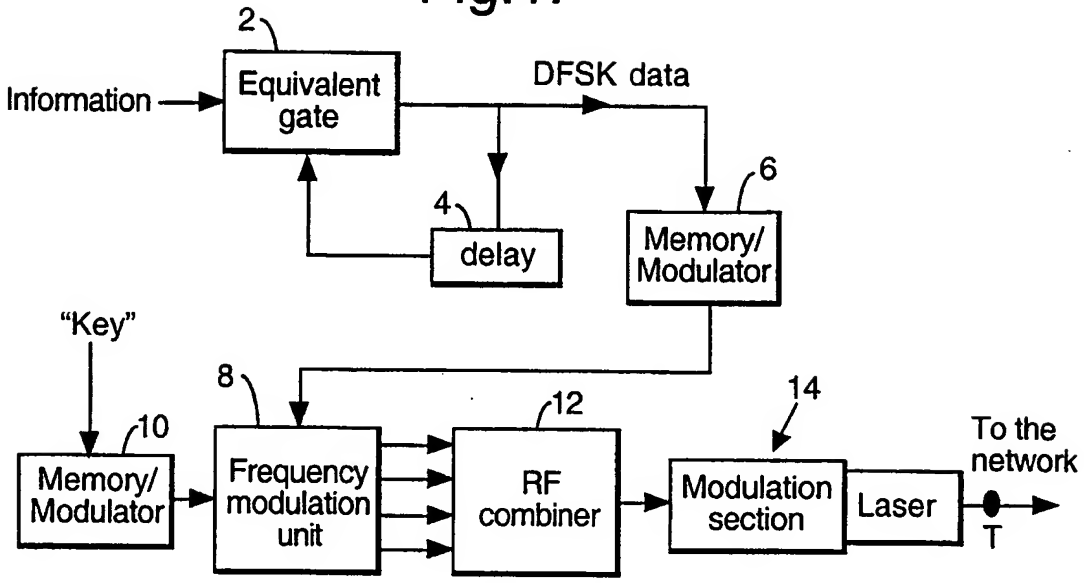

2
Information
Equivalent gate
DFSK data
4
delay
6
Memory/ Modulator
"Key"
8
10
12
14
Memory/ Modulator
Frequency modulation unit
RF combiner
Modulation section
Laser
To the network
T

Fig.2.

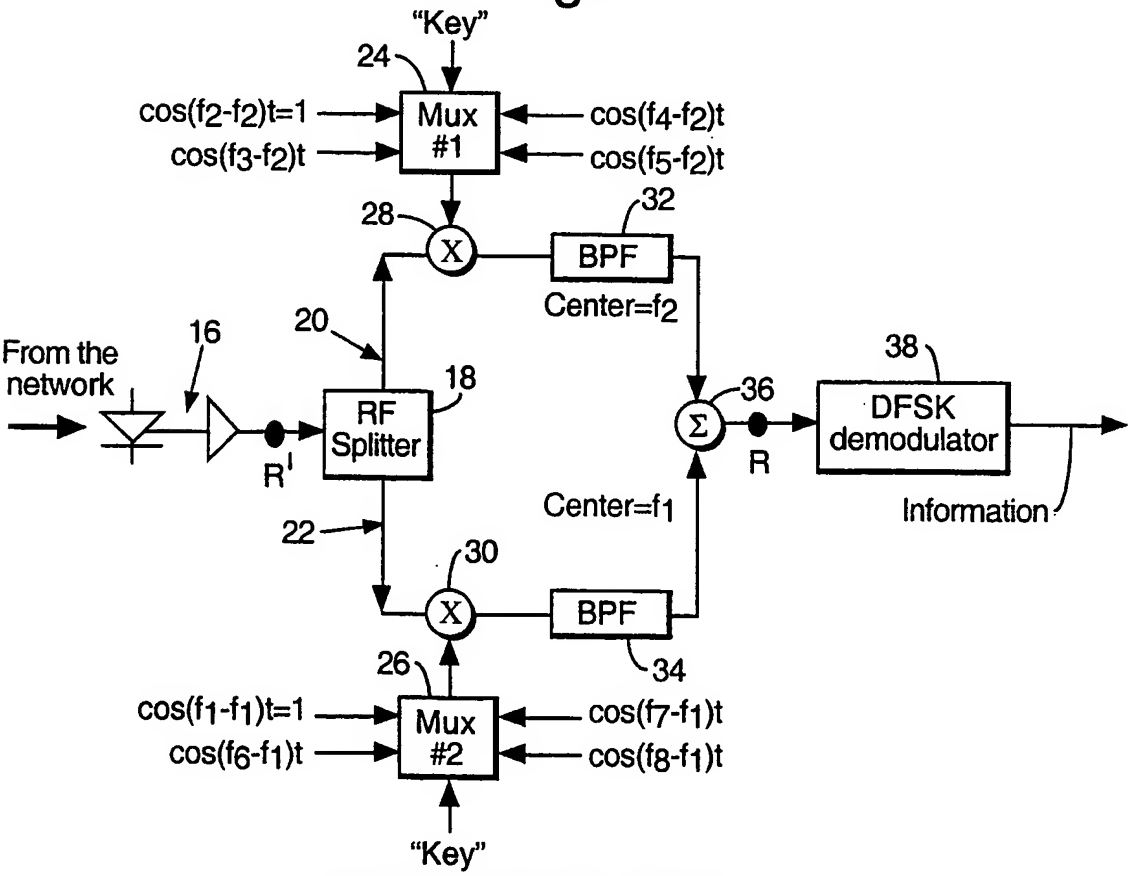

"Key"
24
cos(f2-f2)t=1
cos(f3-f2)t
Mux #1
cos(f4-f2)t
cos(f5-f2)t
28
X
32
BPF
Center=f2
20
16
From the network
18
RF Splitter
R'
38
36
Σ
R
DFSK demodulator
Information
Center=f1
22
30
X
BPF
34
26
cos(f1-f1)t=1
cos(f6-f1)t
Mux #2
cos(f7-f1)t
cos(f8-f1)t
"Key"

Fig.3.

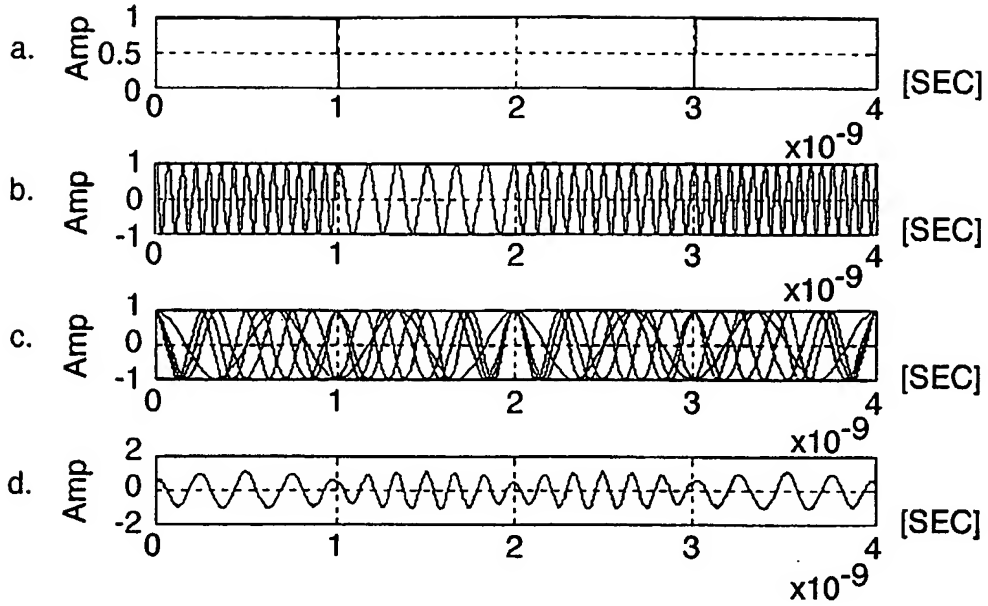


Fig.4.

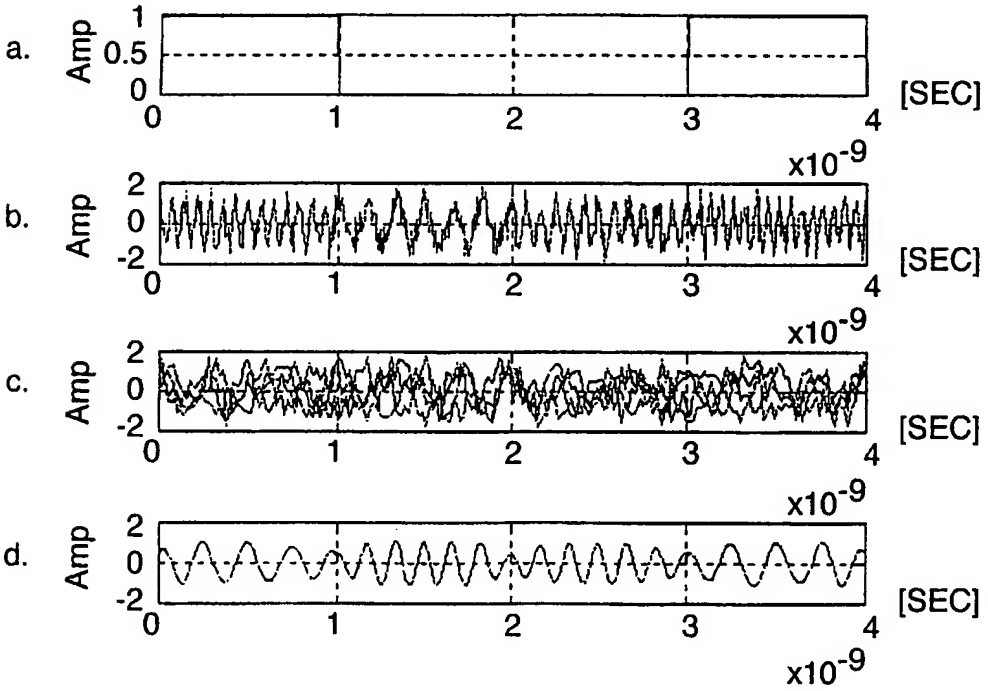


Fig.5.

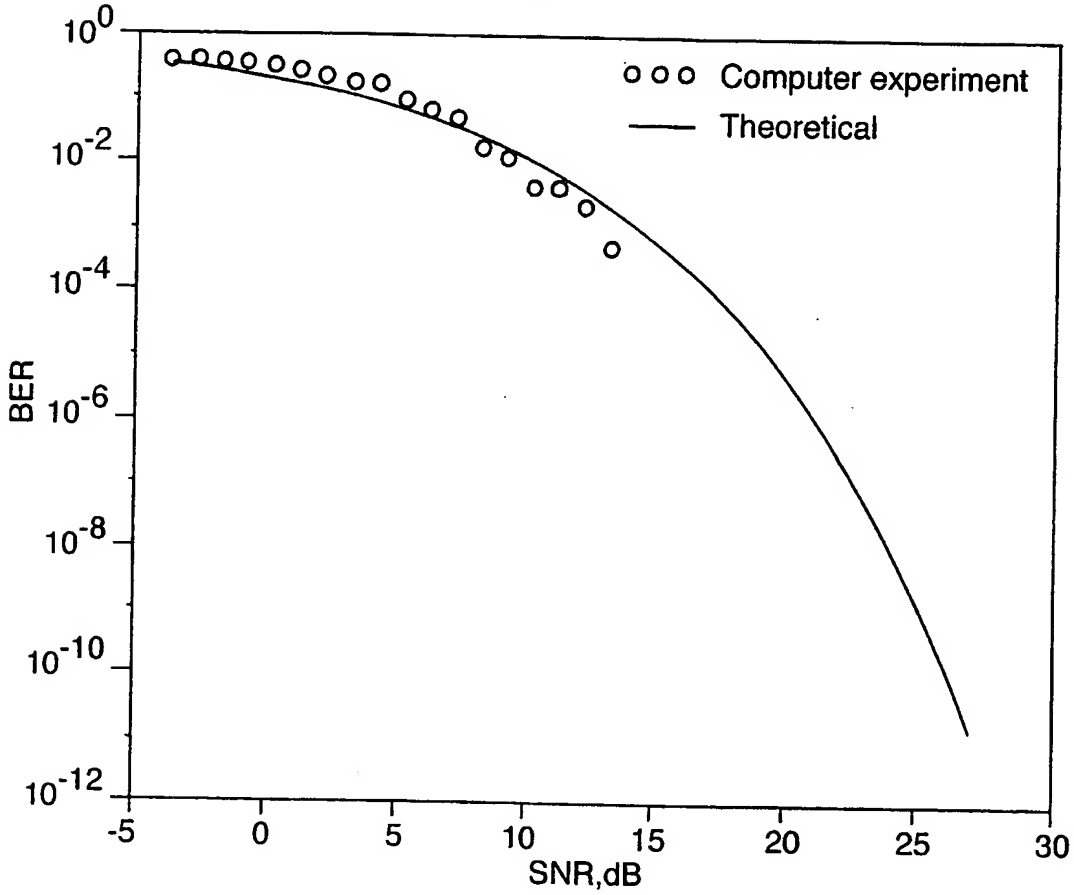

Computer experiment
Theoretical
BER
SNR,dB
10^{0}
10^{-2}
10^{-4}
10^{-6}
10^{-8}
10^{-10}
10^{-12}
-5
0
5
10
15
20
25
30

Fig.6.

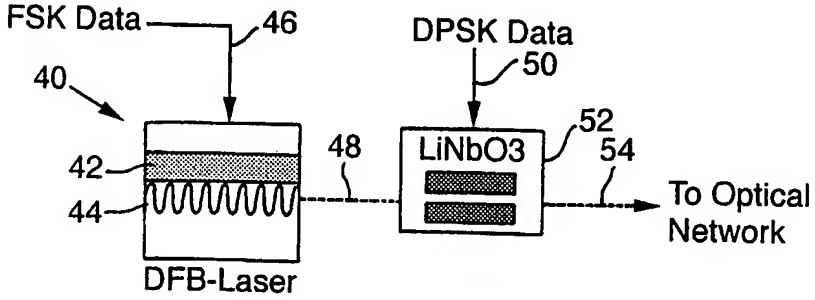

FSK Data
46
DPSK Data
50
40
42
44
48
LiNbO3
52
54
To Optical Network
DFB-Laser

Fig.7.

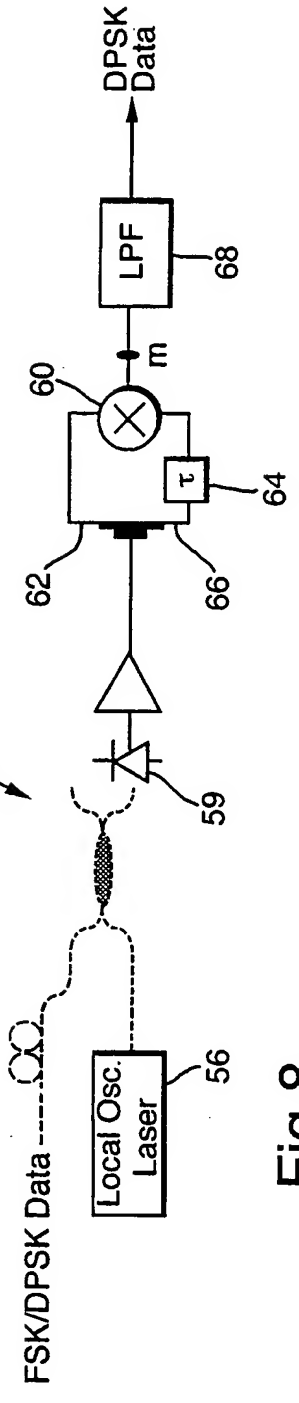


Fig.9.

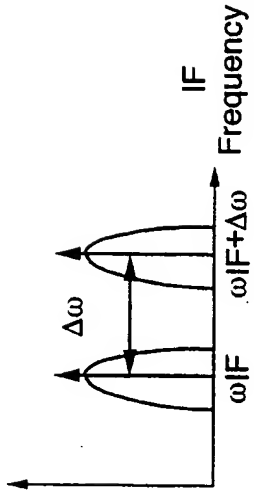


Fig.8.

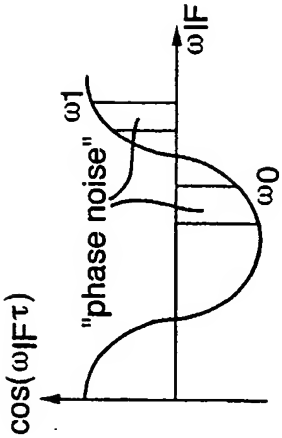


Fig.10.

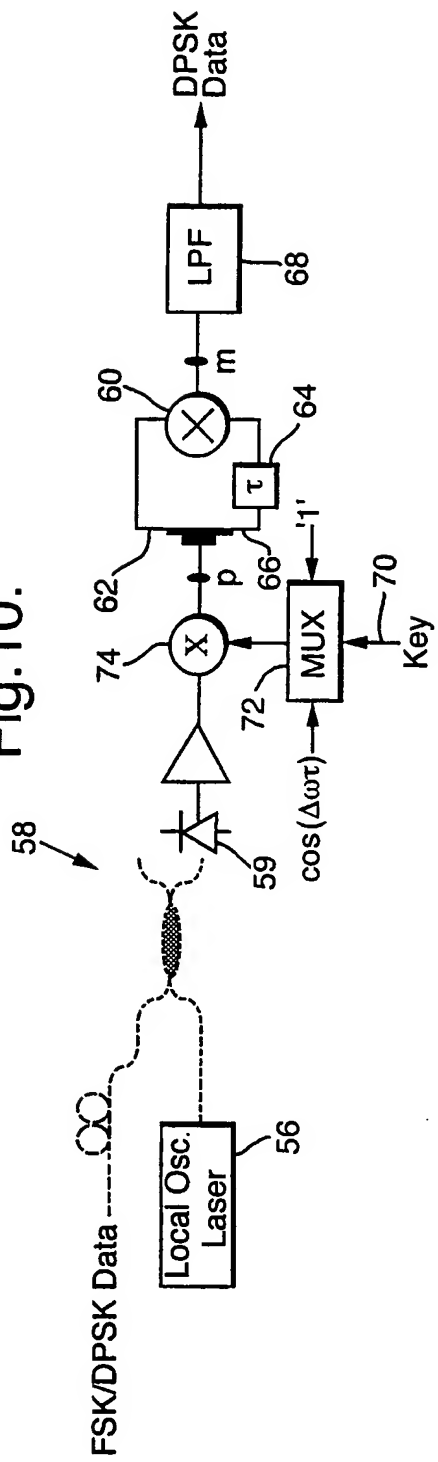


Fig.11.

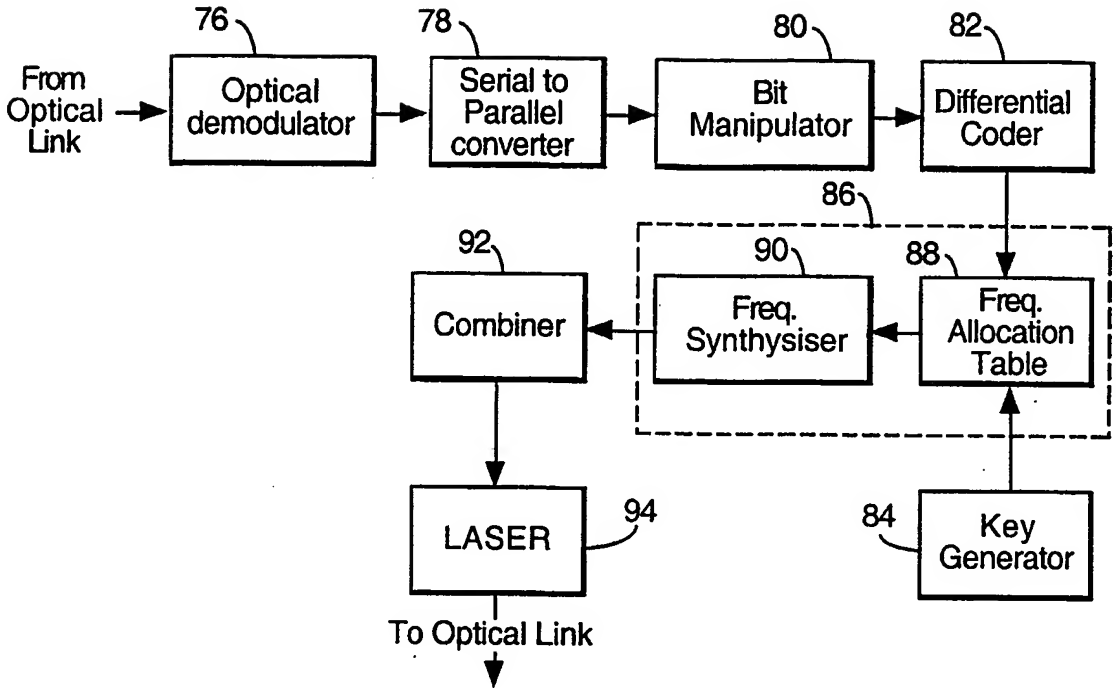
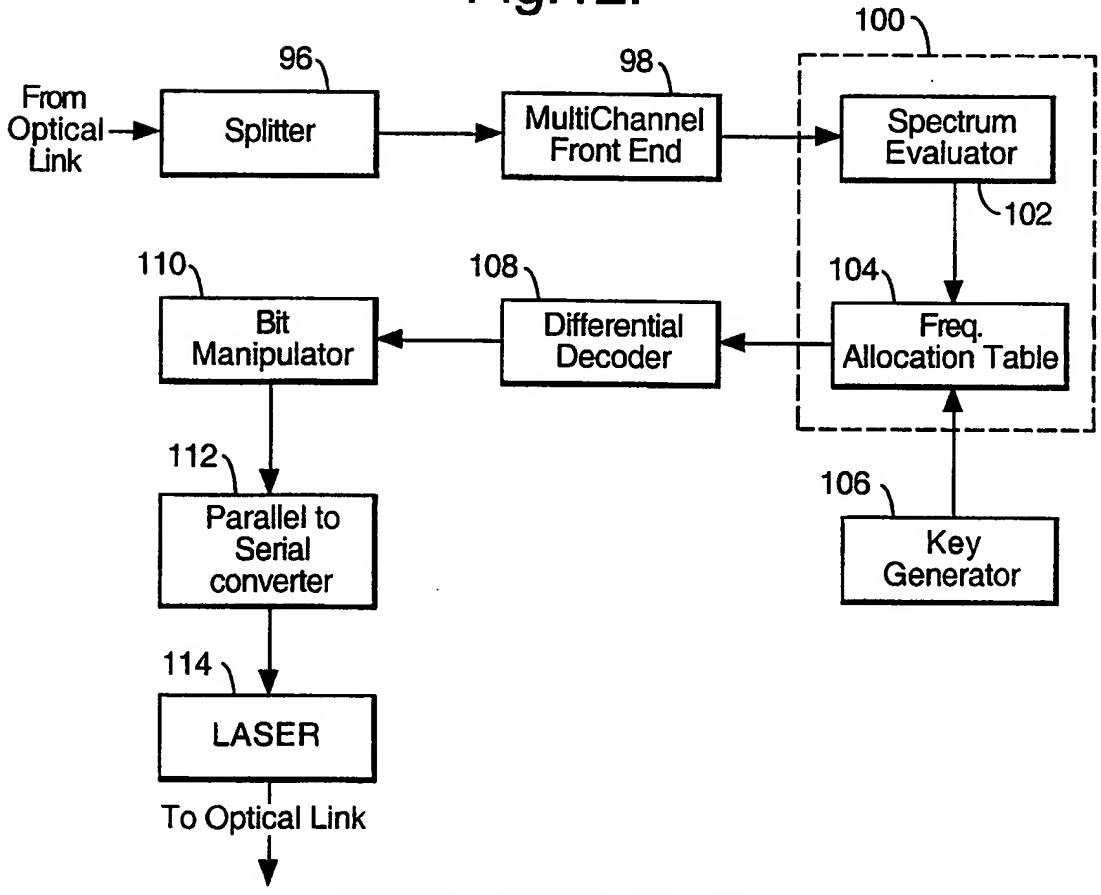

From Optical Link
76
Optical demodulator
78
Serial to Parallel converter
80
Bit Manipulator
82
Differential Coder
86
92
Combiner
90
Freq. Synthysiser
88
Freq. Allocation Table
LASER
94
84
Key Generator
To Optical Link

Fig.12.


From Optical Link
96
Splitter
98
MultiChannel Front End
100
Spectrum Evaluator
102
110
Bit Manipulator
108
Differential Decoder
104
Freq. Allocation Table
112
Parallel to Serial converter
106
Key Generator
114
LASER
To Optical Link